

HDM:BW  
F. #2024R00105

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK  
----- X

UNITED STATES OF AMERICA

- against -

JINJING HE and YUK WONG,

Defendants.

----- X

COMPLAINT AND  
AFFIDAVIT IN SUPPORT  
OF APPLICATION FOR  
ARREST WARRANT

(18 U.S.C. § 1956(h))

24-MJ-159

EASTERN DISTRICT OF NEW YORK, SS:

ALEXANDER VASILIADES, being duly sworn, deposes and states that he is a Special Agent with the Federal Bureau of Investigation (“FBI”), duly appointed according to law and acting as such.

In or about and between June 2022 and September 2022, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants JINJING HE (“HE”) and YUK WONG (“WONG”), together with others, did knowingly and intentionally conspire to conduct one or more financial transactions in and affecting interstate and foreign commerce, to wit: electronic money transfers, in and affecting interstate and foreign commerce, by, through and to one or more financial institutions; in criminally derived property that was of a value greater than \$10,000 and that was derived from specified unlawful activity, to wit: wire fraud, in violation of Title 18, United States Code, Section 1343, all contrary to Title 18, United States Code, Section 1957(a).

(Title 18, United States Code, Section 1956(h) and 3551 et seq.)

The source of your deponent's information and the grounds for his belief are as follows:<sup>1</sup>

1. I am a Special Agent with the FBI and have been since March 2020. Previously, I was a Special Agent with the United States Secret Service for over three years. As a Special Agent, I am responsible for conducting and assisting in investigations into the activities of individuals and criminal groups responsible for financial crimes and related offenses. I have participated in investigations involving the review of information seized from electronic communication accounts and electronic devices, debriefing of victims, review of telephone records and global positioning system ("GPS") data, review of money transfer records, surveillance, analysis of pen register information, and other investigative techniques. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities, including the manner in which criminals use email, telephone calls, text messages, electronic communications and cloud-based data storage accounts to perpetrate fraudulent schemes.

#### Overview of the Money Laundering Scheme

2. Since June 2022, the defendants JINJING HE and YUK WONG, together with others, have received the proceeds of fraud victims into bank accounts controlled by them, and then transferred the fraud proceeds to other accounts in order to conceal the source of the funds. As part of their money laundering activities, HE and WONG have engaged in a pattern of consistent conduct across multiple victims. For example, HE and WONG have regularly

---

<sup>1</sup> Because the purpose of this Complaint is to set forth only those facts necessary to establish probable cause to arrest, I have not described all the relevant facts and circumstances of which I am aware.

opened bank accounts days or weeks before receiving large sums of money from fraud victims who have no connection to HE and WONG. The bank accounts have nearly no activity other than the receipt of victim funds and the immediate transfer of those funds to bank accounts in a manner consistent with money laundering. Consistently, the funds received by HE and WONG are ultimately transferred to bank accounts outside the United States. The bank accounts are kept open only for a couple of months before they are closed.

3. HE and WONG have also fabricated multiple contracts between companies they have set up to receive fraud victims' funds and the fraud victims. These purported contracts, which are substantively similar to one another but span multiple fraud victims, are intended to conceal the illicit nature of the funds HE and WONG have received and transferred.

Victim 1

4. In or about June 2022, Victim 1, an individual whose identity is known to me, and lives in the Eastern District of New York began communicating via Facebook and WhatsApp with an individual who identified herself as "Arlena." Arlena claimed to work at a Hong Kong company that was going to be awarded a contract to provide data backup services to a Singapore-based cryptocurrency exchange called Priviumex. Arlena subsequently told Victim 1 that her company had been awarded the contract and that, in the process of performing data backup for Priviumex, she had noticed that one Priviumex client had over \$100 million worth of cryptocurrency in three Priviumex accounts.

5. Arlena told Victim 1 that she told her boss about this client's holdings and her boss suggested that they follow the client's trading patterns in an attempt to make money in the cryptocurrency markets. Arlena subsequently told Victim 1 that she and her boss both

invested \$50,000 worth of cryptocurrency on Priviumex and that she had made a 13% profit by following the client's trading strategy. Arlena later told Victim 1 that she had invested even more money on Priviumex and sent Victim 1 screenshots purporting to show that she had made approximately \$1.4 million in profits.

6. Victim 1 subsequently asked Arlena to make trades on Victim 1's behalf. Arlena refused, but instead sent Victim 1 a link to download the Priviumex mobile application and instructed Victim 1 to link his/her Coinbase account to his/her Priviumex account. In connection with the registration of his/her Priviumex account, Victim 1 submitted a photograph of his/her driver's license to Priviumex. Arlena then introduced Victim 1 to a purported Priviumex customer service representative, who would help Victim 1 execute trades on Priviumex. The customer service representative then instructed Victim 1 to wire the money Victim 1 wanted to invest to various U.S.-based bank accounts.

7. On or about July 27, 2022, Victim 1 made two wire transfers in the amounts of \$200,000.00 and \$101,000.00 to a JP Morgan Chase bank account in the name of Lucky XC Trading Inc. (Lucky XC Trading Inc. is hereinafter referred to as "Lucky XC"; the Lucky XC JP Morgan Chase account is hereinafter referred to as the "Chase Lucky XC" account"). Prior to these transfers, the Chase Lucky XC account had a balance of \$100.

8. Lucky XC Trading Inc. ("Lucky XC") is a "domestic business corporation" registered with the New York Department of State. Lucky XC was founded and filed its registration paperwork on July 6, 2022, approximately three weeks before Victim 1's first two transfers into the Chase Lucky XC account. According to its New York Department of State registration, the defendants JINJING HE and YUK WONG are the only registered agents of Lucky XC.

9. The Chase Lucky XC account was opened on or about July 8, 2022, less than three weeks before Victim 1's first two transfers into the account. Records obtained from Chase indicate that the defendant YUK WONG is identified as the President and the signatory of the Chase Lucky XC account. On or about July 13, 2022, the defendant JINJING HE replaced WONG as the President and signatory of the Chase Lucky XC account.

10. On or about July 28, 2022—one day after Victim 1 transferred \$301,000 to the Chase Lucky XC account, the Chase Lucky XC account transferred \$300,750.00 to a Signature bank account in the name of UKDE Limited ("UKDE"), which is registered to an individual located in the United Kingdom.

11. On or about July 25, 2022, UKDE—the company to which the Chase Lucky XC account transferred Victim 1's funds on or about July 28, 2022—was provided with "Know Your Client" information relating to Lucky XC. Specifically, UKDE was provided with a photo of the defendant JINJING HE in which he was holding his New York driver's license<sup>2</sup>, a photo of HE's United States passport, a copy of Lucky XC's New York Department of State registration filing, a copy of Lucky XC's Articles of Association.

12. In addition, on or about July 25, 2022, UKDE was provided with a purported "Purchase Contract" between Lucky XC and Victim 1, dated July 22, 2022. The "Purchase Contract" purported to memorialize a sale by Lucky XC to Victim 1 of 5,000 units of "Clothes" for \$301,000, the same amount that Victim 1 wired to the Chase Lucky XC account on or about July 27, 2022. The "Purchase Contract" claims to be signed by Victim 1. However, in

---

<sup>2</sup> Based on a review of New York State Department of Motor Vehicle records, it appears that HE altered the ID number on the driver's license in the photo submitted to UKDE. In the photo submitted to UKDE, the driver's license ID is 872-950-612. Based on DMV records, the actual ID number on HE's license is 875-960-215.

an interview with law enforcement officers, Victim 1 reviewed the “Purchase Contract” and stated that he/she had never previously seen the contract and did not sign the contract. Rather, the signature included on the “Purchase Contract” appears to be identical to the signature on Victim 1’s driver’s license, a copy of which Victim 1 provided to Priviumex when Victim 1 was setting up his/her Priviumex account. Victim 1 advised that he/she no longer signs documents in the same manner as he/she signed the driver’s license, and my review of more recent bank records signed by Victim 1 confirms that his/her signature in 2022 differed substantially from the signature on his/her driver’s license. Thus, it appears that the signature on Victim 1’s driver’s license, which was provided to Priviumex, was then provided to Lucky XC and appended to the “Purchase Contract” purportedly entered into by Lucky XC and Victim 1.

13. Similarly, on or about July 29, 2022, UKDE was provided with a purported “International Trade Contract” dated July 22, 2022 between Lucky XC and Victim 1. The “International Trade Contract” purported to memorialize a sale by Lucky XC to Victim 1 of 10,000 units of “Sport suit” for \$178,600 and 10,000 units of “Sports shoes” for \$122,400, which totals \$301,000, the same amount that Victim 1 wired to the Chase Lucky XC account on or about July 27, 2022. The “International Trade Contract” claims to be signed by Victim 1. In an interview with law enforcement officers, Victim 1 reviewed the “International Trade Contract” and stated that he had never previously seen the contract and did not sign the contract.

14. On or about August 10, 2022, Victim 1 made another wire transfer of \$400,000.00 to the Chase Lucky XC account, and another individual transferred \$50,000.00 to the Chase Lucky XC account. Prior to these transfers, the Chase Lucky XC account had a balance of \$315. On or about August 11, 2022, the Chase Lucky XC account transferred

\$449,180.00—nearly all of the money transferred by Victim 1 and the other individual the previous day—to the same UKDE Limited account.

15. On or about August 12, 2022, UKDE was provided with another purported “Purchase Contract” between Lucky XC and Victim 1. This “Purchase Contract” is substantively identical to the “Purchase Contract” described in paragraph 12. The “Purchase Contract” purported to memorialize a sale by Lucky XC to Victim 1 of 10,000 units of “Sport Shoes” for \$400,000, the same amount that Victim 1 wired to the Chase Lucky XC account on or about August 10, 2022. The “Purchase Contract” claims to be signed by Victim 1. In an interview with law enforcement officers, Victim 1 reviewed the “Purchase Contract” and stated that he had never previously seen the contract and did not sign the contract.

16. Subsequent to making these wire transfers, Victim 1 became unable to access his/her funds on Priviumex. Victim 1 was told by a Priviumex customer service representative that he/she would only be able to access his/her funds if he/she paid a 10% penalty fee. Arlena provided Victim 1 with a bank account to wire the 10% fee and Victim 1 wired a total of \$209,756.00 to this bank account. After wiring these funds, Arlena told Victim 1 that she could transfer back to Victim 1 a portion of his/her funds, but only if he/she agreed to wire more money in fees. At this point, Victim 1 realized he/she had been a victim of fraud and ceased communicating with Arlena.

#### Victim 2

17. In or about June 2022, Victim 2 began communicating on Instagram and WhatsApp with an individual identifying herself as “Lisa,” who claimed to live in Singapore. Lisa began talking to Victim 2 about cryptocurrency investing and told Victim 2 that she invests in cryptocurrency in her spare time.

18. Lisa instructed Victim 2 to download an application called Bitget and provided Victim 2 with a link to download Bitget.<sup>3</sup> Lisa began coaching Victim 2 on when to make cryptocurrency trades. Victim 2 was provided with bank accounts and instructed to wire funds to those bank accounts in order to facilitate faster trades and realize profits more quickly.

19. One of the bank accounts Lisa provided Victim 2 was the Chase Lucky XC account. At Lisa's direction, on or about August 29, 2022, Victim 2 wired \$220,000.00 to the Chase Lucky XC account. Prior to this transfer, the Chase Lucky XC account had a balance of \$15.98.

20. On or about August 30, 2022, the Chase Lucky XC account transferred \$218,200.00—nearly all the money Victim 2 had wired the Chase Lucky XC account the previous day—to a bank account registered at Silvergate Bank in California.

21. After Victim 2 transferred the \$220,000.00 to the Chase Lucky XC account, Victim 2 attempted to withdraw his/her funds, but was unable to. Rather, Victim 2 was told that in order to remove his/her funds, he/she would have to pay an additional \$300,000.00 to “verify” his/her identity due a supposed security breach on Bitget. At that point, Victim 2 realized he/she had been a victim of fraud and did not make this payment.

WHEREFORE, your deponent respectfully requests that the defendant JINJING HE and YUK WONG be dealt with according to law.

It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the Affidavit and Arrest Warrant. I believe that sealing these documents is necessary because they are relevant to

---

<sup>3</sup> Bitget is a legitimate cryptocurrency exchange platform. Based on our investigation, it appears that the link Lisa sent Victim 2 was not a link to download the legitimate Bitget app, but rather a link to download a spoofed, or fake, version of Bitget.



an ongoing criminal investigation, which is not public at this time. Premature disclosure of the contents of this Affidavit and the related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness, and could result in a risk of flight by the defendant.



ALEXANDER VASILIADES  
Special Agent, Federal Bureau of Investigation

Sworn to before me by telephone  
this \_\_22\_\_ day of February 2024.



THE HONORABLE LOIS BLOOM  
UNITED STATES MAGISTRATE JUDGE  
EASTERN DISTRICT OF NEW YORK